IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor:	Roskind et al	Examiner:	Sims, Jing F.
Application No.:	11/237,003	Art Unit:	4148
Filed:	9/27/2005	Docket No.:	PB-034
Title:	CONTAGION ISOLATION AND INOCULATION		

CERTIFICATE OF FILING

I hereby certify that this correspondence is being electronically filed on: July 19, 2011.

/Aaron T. Emigh/
Aaron Emigh

APPELLANT'S BRIEF PURSUANT TO 37 C.F.R. §41.37

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Appellant, Applicant in the above-captioned patent application and Manager of Radix Holdings, LLC, the assignee of record, appeals the final rejection of Claims 1, 2, 4-10, 12-14, 24, and 25 set forth in the final Office Action mailed on July 20, 2010.

I. REAL PARTY IN INTEREST

The real party of interest in the present application is Radix Holdings, LLC, the assignee of record.

II. RELATED APPEALS AND INTERFERENCES

PURSUANT TO 37 C.F.R. §41.37(c)(1)(ii), Appellant hereby notifies the Board of Patent Appeals that Appellant and the Assignee do not know of any appeals or interferences that will directly affect or be directly affected by or have any bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1, 2, 4-10, 12-14, 24, and 25 are currently pending in the application, and are attached hereto as an appendix. Claims 3, 11, 15-23, 26, and 27 have been canceled. All pending claims were finally rejected by the Examiner and are the subject of this appeal.

IV. STATUS OF AMENDMENTS

All Amendments as of Appellant's Amendment B, filed on January 10, 2010, are believed to have been entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Since the application is being prosecuted *pro se*, a summary of claimed subject matter is not required according to 37 CFR 41.37(c)(1).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1, 2, 4-10, and 12-14 are anticipated under 35 USC 102(e) by Liang (US 7,872,278).

Whether claim 24 is unpatentable under 35 USC 103(a) over Liang in view of Lewis et al (US Pub. No. 2005/0131997), hereinafter referred to as Lewis.

Whether claim 25 is unpatentable under 35 U.S.C. 35 USC 103(a) over Liang in view of McElhaney, Jr., et al (US Patent No. 6,823,479 B1), hereinafter referred to as McElhaney.

VII. ARGUMENT

WHETHER CLAIMS 1, 2, 4-10, AND 12-14 ARE ANTICIPATED UNDER 35 USC 102(E) BY LIANG

For the reasons set forth below, Appellant respectfully submits that the Examiner has erred in maintaining the 35 U.S.C 102(e) rejection of Claims 1, 2, 4-10, and 12-14.

The MPEP, §2131, states that in order for a rejection under 35 USC 102 to be proper, "'The identical invention must be shown in as complete detail as is contained in the ... claim.' *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)." As will be shown below, Liang does not show the identical invention in complete detail, and therefore the Examiner erred in his rejection under 35 USC 102(e).

Claims 1, 9, and 14

Liang does not anticipate "detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness," nor "when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network," as recited in amended independent claims 1 and 14, and similarly in amended independent claim 9.

Liang does not teach "wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host" because Liang does not teach either a trusted computing base or a trusted platform module.

The Examiner has cited Liang, column 8, lines 49-53 as anticipating "wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host," as recited in claims 1, 9, and 14. However, the cited

passages of Liang read "For example, virus monitor 102-1 sends a query 140 *to each of the client devices* 110-116 requesting confirmation that each has installed therein the appropriate anti-virus software as determined by the policies contained in the OPP file 135…" (Liang, column 8, lines 49-53, emphasis added.) Nothing in this, or elsewhere in Liang, appears to teach or suggest "contacting a trusted computing base," nor "a trusted computing base associated with a trusted platform module within the first host," as recited in claims 1, 9, and 14.

"Trusted computing base" and "trusted platform module are terms of art with specific meanings that are in no way discussed in Liang. The Wikipedia entry for "Trusted Platform Module (http://en.wikipedia.org/wiki/Trusted_platform_module; retrieved January 10, 2010) begins, "In computing, Trusted Platform Module (TPM) is both the name of a published specification detailing a secure cryptoprocessor that can store cryptographic keys that protect information, as well as the general name of implementations of that specification, often called the "TPM chip" or "TPM Security Device" (as designated in certain Dell BIOS settings[1]). The TPM specification is the work of the Trusted Computing Group. The current version of the TPM specification is 1.2 Revision 103, published on July 9, 2007." Reinforcing the industry adoption of this technology and standardization around the term of art used in the claims, this specification has also been adopted as ISO/IEC standard 11889. As for the term of art "trusted computing base," the final paragraph of the "Definition and characterization" section of the Wikipedia entry on "Trusted Computing Base" (http://en.wikipedia.org/wiki/Trusted_computing_base; retrieved January 10, 2010) states that "A given piece of hardware or software is a part of the TCB if and only if it has been designed to be a part of the mechanism that provides its security to the computer system."

Liang does not anticipate a trusted platform module, nor a trusted computing base associated with a trusted platform module. Indeed, Appellant discussed the previously presented amendment to claims 1, 9, and 14 with the Examiner and Supervisory Patent Examiner Emmanuel Moise on April 14, 2009. During that interview, the Examiner explicitly stated that she believed the language in these claims as amended in Amendment A and presented herein overcame Liang, as indeed, they appear to do.

However, in the Final Office Action, the Examiner acknowledged Appellant's argument that Liang does not teach these terms of art, but further argued that because Liang vaguely states that "any operating system" may be used, that this anticipates operating systems with trusted platform modules and a trusted computing base. This argument is erroneous on at least two counts. First, it is erroneous because a trusted platform is a hardware component and not merely an operating system component. Second, it is erroneous because *Liang does not actually teach these limitations*, nor does the Examiner argue that it does. As noted above, the *Suzuki* standard for a §102 rejection is that "the identical invention must be shown ***in as complete detail as is contained in the ... claim***." (Emphasis added.) Clearly, Liang does not disclose the detail in the claim, i.e. "a trusted computing base associated with a trusted platform module,"and therefore it cannot anticipate under 35 USC 102(e).

Liang does not teach "determining whether the response includes a valid digitally signed attestation of cleanliness."

The Examiner has cited Liang, column 8, lines 53-55 as anticipating "determining whether the response includes a valid digitally signed attestation of cleanliness." The cited section of Liang reads "Upon receiving the query 140, each of the client devices checks for confirmation that the appropriate anti-virus software is indeed present." This, as elsewhere in Liang, does not appear to teach or suggest a "valid digitally signed attestation of cleanliness."

Similarly, the Examiner has cited Liang, column 8, lines 55-59 as anticipating "when it is determined that the response does not include a valid digitally signed attestation of cleanliness." The cited section of Liang reads "If, say in the case of the client device 116, that [sic] it is determined that either no software is present or the installed software is not appropriate (based upon the policies of the OPP file 135, for example), the client device 116 is directed only to the anti-virus software installation server 138 and no other..." This, as elsewhere in Liang, does not appear to teach or suggest a "valid digitally signed attestation of cleanliness."

In response to Appellant's observation that Liang does not teach "a valid digitally signed attestation of cleanliness," the Examiner responded that "in a Linux equipped with trusted computing system [sic], the confirmation is in 'upon receiving the query 140, each of the client

device [sic] check for confirmation that the appropriate antivirus software is indeed present' (Liang: col. 8, lines 53-59) is [sic] corresponding to valid digitally signed attestation."

Again, the *Suzuki* standard for a §102 rejection is that "the identical invention must be shown ***in as complete detail as is contained in the ... claim***." (Emphasis added.) Clearly, since Liang does not disclose the detail in the claim, i.e. "a valid digitally signed attestation," and the Examiner is instead speculating as to what a "confirmation" might be that is *not* disclosed in Liang, it cannot anticipate under 35 USC 102(e).

The use of a trusted computing base, trusted platform module, and valid digitally signed attestation of cleanliness in detecting an insecure condition are significant innovations, as they can, for example, prevent false reports by ensuring that an attestation of cleanliness is reliable and the result of properly executed checks. Without the use of such techniques, approaches such as Liang are potentially vulnerable to false reports by infected machines, and may fail to quarantine such machines, resulting in higher infection rates and greater propagation of malicious software.

The Examiner has erred by improperly reading into Liang extremely innovative applications that are simply not taught by it. In doing so, the Examiner has improperly rejected claims 1, 9, and 14 under 35 USC 102(e).

Claims 2 and 4-8

Claims 2 and 4-8 depend from claim 1. As discussed above, the Examiner's rejection of claim 1 under 35 USC 102(e) was erroneous. The Examiner relied on this erroneous rejection in the rejections of claims 2 and 4-8. Therefore, the rejections of claims 2 and 4-8 are also erroneous.

Claims 10, 12, and 13

Claims 10, 12, and 13 depend from claim 9. As discussed above, the Examiner's rejection of claim 9 under 35 USC 102(e) was erroneous. The Examiner relied on this erroneous rejection in the rejections of claims 10, 12, and 13. Therefore, the rejections of claims 10, 12, and 13 are also erroneous.

WHETHER CLAIM 24 IS UNPATENTABLE UNDER 35 USC 103(A) OVER LIANG IN VIEW OF LEWIS

For the reasons set forth below, Appellant respectfully submits that the Examiner has erred in maintaining the 35 U.S.C 103(a) rejection of Claim 24.

Claim 24

Claim 24 depends from claim 1. As discussed above, the Examiner's rejection of claim 1 under 35 USC 102(e) was erroneous. The Examiner relied on this erroneous rejection in the rejections of claim 24. Therefore, the rejection of claim 24 is also erroneous.

WHETHER CLAIM 25 IS UNPATENTABLE UNDER 35 U.S.C. 35 USC 103(A) OVER LIANG IN VIEW OF MCELHANEY

For the reasons set forth below, Appellant respectfully submits that the Examiner has erred in maintaining the 35 U.S.C 103(a) rejection of Claim 25.

Claim 25

Claim 25 depends from claim 1. As discussed above, the Examiner's rejection of claim 1 under 35 USC 102(e) was erroneous. The Examiner relied on this erroneous rejection in the rejections of claim 25. Therefore, the rejection of claim 25 is also erroneous.

VIII. CLAIMS APPENDIX

1. A method for protecting a network, comprising:

detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network; and

permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition.

2. A method as recited in claim 1, wherein detecting an insecure condition further includes at least one of the following: scanning for a vulnerability, scanning for malicious data, checking a configuration or setting, determining whether a security data is up to date, determining whether a security software is installed, detecting anomalous network traffic, and determining that an available patch has not been installed.

4. A method as recited in claim 1, wherein detecting an insecure condition includes determining that the first host should be quarantined until an update to an operating system has been installed.

5. A method as recited in claim 1, wherein detecting an insecure condition includes configuring an operating system to quarantine the first host upon initial startup after installation of the operating system.

6. A method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes:

detecting an outbound communication from the first host; and

forwarding the outbound communication if it is addressed to a remediation host.

7. A method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes:

detecting an outbound communication from the first host; and

redirecting the outbound communication to a quarantine server if it comprises a request for an approved service and is not addressed to a remediation host.

8. A method as recited in claim 1, wherein quarantining the first host further includes preventing the first host from receiving via the protected network data not related to remediation of the insecure condition.

9. A system for protecting a network, comprising:

a processor configured to:

detect an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantine the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network; and

permit the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition; and

a memory coupled to the processor and configured to provide instructions to the processor.

10. A system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by performing one or more of the following: scanning for a vulnerability, scanning for malicious data, checking a configuration or setting, determining whether a security data is up to date, determining whether a security software is installed, detecting anomalous network traffic, determining that an available patch has not been installed, and querying the first host for a cleanliness assertion.

12. A system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by determining that an initial startup after installation of an operating system is being performed.

13. A system as recited in claim 9, wherein the processor is configured to quarantine the first host at least in part by preventing the first host from receiving via the protected network data not related to remediation of the insecure condition.

14. A computer program product for protecting a network, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for:

detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network; and

permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition.

24. A method as recited in claim 1, further comprising:

receiving a service request sent by the first host;

serving a quarantine notification page to the first host if the service request comprises a web server request; and

in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host.

25. A method as recited in claim 1, performed at an Internet service provider.

IX. EVIDENCE APPENDIX

Not Applicable.

X. RELATED PROCEEDINGS APPENDIX

Not Applicable.

Respectfully submitted,

Dated: July 19, 2011

/Aaron T. Emigh/
Aaron Emigh
Customer #85853